Self-Policing Mobile Ad Hoc Networks by Reputation Systems

Sonja Buchegger, University of California at Berkeley
Jean-Yves Le Boudec, EPFL-IC-LCA

ABSTRACT

Node misbehavior due to selfish or malicious reasons or faulty nodes can significantly degrade the performance of mobile ad hoc networks. To cope with misbehavior in such self-organized networks, nodes need to be able to automatically adapt their strategy to changing levels of cooperation. Existing approaches such as economic incentives or secure routing by cryptography alleviate some of the problems, but not all. We describe the use of a self-policing mechanism based on reputation to enable mobile ad hoc networks to keep functioning despite the presence of misbehaving nodes. The reputation system in all nodes makes them detect misbehavior locally by observation and use of second-hand information. Once a misbehaving node is detected it is automatically isolated from the network. We classify the features of such reputation systems and describe possible implementations of each of them. We explain in particular how it is possible to use second-hand information while mitigating contamination by spurious ratings.

MISBEHAVIOR IN MOBILE AD HOC NETWORKS

In mobile ad hoc networks, nodes are both routers and terminals. For lack of routing infrastructure, they have to cooperate to communicate. Cooperation at the network layer means routing (i.e., finding a path for a packet) and forwarding (i.e., relaying packets for others).

Misbehavior means deviation from regular routing and forwarding. It arises for several reasons; unintentionally when a node is faulty. Intentional misbehavior can aim at an advantage for the misbehaving node or just constitute vandalism, such as enabling a malicious node to mount an attack or a selfish node to save power. In game-theoretic terms, cooperation in mobile ad hoc networks poses a dilemma. To save battery, bandwidth, and processing power, nodes should not forward packets for others. If this dominant strategy is adopted, however, the outcome is a nonfunctional network when multihop routes are needed, so all nodes are worse off.

Without countermeasures, the effects of misbehavior have been shown to dramatically decrease network performance [1, 2]. Depending on the proportion of misbehaving nodes and their strategies, decreased network throughput , packet loss, denial of service, and network partioning can result. These detrimental effects of misbehavior can endanger the entire network. Unless misbehavior is addressed to provide reliable and trustworthy ad hoc networks, users might be reluctant to use them.

The question we address is, how can we make an existing system keep working despite misbehavior? Can one weed out misbehaving nodes? When fewer nodes deviate from the protocol, network performance is more predictable and less chaotic.

The main solutions to address this question are secure routing, economic incentives, and detection and reputation systems. Secure routing using cryptography, such as Ariadne or Secure Routing Protocol (SRP) [3], provides prevention against specific malicious attacks (e.g., compromising routes). Secure routing applies to route discovery. Once a route is found, its use is not secured.

Economic incentives such as payment schemes aim at making selfish nodes forward for others despite the power usage and effort this entails. Nodes are paid for forwarding, and pay for the forwarding of their own packets by other nodes. An example are nuglets, a virtual currency, or the credit counter [3] in secure hardware, where nodes keep track of remaining battery power and credit. These approaches make it undesirable for selfish nodes to deny forwarding. They do not, however, target other types of misbehavior.

Secure routing and economic incentives solve part of the question, but not all. There remain various observable types of misbehavior that cannot be cured easily, such as silent route changes, which may be addressed by detection and reputation systems. They monitor and rate the behavior of other nodes in routing and forwarding such that nodes can respond according to their opinion about other nodes. The opinion a node has of another is called *reputation*. The goal of a reputation system is to enable nodes to make informed decisions about which nodes to cooperate with or exclude from the

The work presented in this article was supported (in part) by the National Competence Center in Research on Mobile Information and Communication Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322.

0163-6804/05/$20.00 © 2005 IEEE

Monitoring, reputation, and response come at the price of overhearing transmissions of others, keeping a reputation rating about nodes of interest, and updating it at each observation. The gain can be measured in increased throughput and decreased number of lost packets.

network. Reputation systems can be used to cope with any kind of misbehavior as long as it is observable.

We next describe a framework for detection and reputation systems, and list a number of proposed approaches. Then we analyze the main issues and features for reputation systems, which we define as representation of information and classification, use of second-hand information, trust, and redemption and secondary response. In separate sections we discuss how each of these features can be implemented, using one such reputation system as a basis for comparison. We explain in particular how it is possible to use second-hand information while mitigating contamination by spurious ratings. Then we illustrate on some scenarios the types of misbehavior targeting reputation systems.

Detection and Reputation Systems

The goal of a detection and reputation system is to enable nodes to adapt to changes in the network environment caused by misbehaving nodes. This is achieved by the following functions.

Monitoring

The goal of monitoring is to gather first-hand information about the behavior of nodes in the network. Monitoring systems detect misbehavior that can be distinguished from regular behavior by observation.

Not forwarding is just one of the possible types of misbehavior in mobile ad hoc networks. Several others, mostly concerned with routing rather than forwarding, have been suggested (e.g., black hole routing, gray hole routing, worm hole routing). We classify misbehavior types as packet dropping, modification, fabrication, or timing misbehavior; many of these can be detected by direct observation, as we have shown in a testbed implementation [4].

To detect misbehavior, nodes take into account the packets they receive (e.g., a received acknowledgment from the destination means that all the nodes on the route cooperated in forwarding); they can also use enhanced passive acknowledgments (PACKs) by overhearing the transmissions of the next hop on the route, since they are within range when using omnidirectional antennas. For instance, if they do not overhear a retransmission to the following node within a timeout of, say, 100 ms, or the overheard transmission shows that the packet header has been illegitimately modified, they conclude misbehavior. To distinguish from physical failures of the next hop, the timeout allows for retransmission attempts if the transmission of the next hop fails. If there are link failures over a longer time, the node can expect a route error (RERR). To account for connectivity problems at the monitoring node itself, it disregards PACK timeouts in the case of link-layer error messages received from its own interface.

In addition to a list of known types of misbehavior, nodes can automatically learn about new misbehavior in analogy to the human immune system [5].

Reputation

Reputation systems are used for example in some on-line auctioning systems. They provide a means of obtaining a quality rating of participants of transactions by having the buyer and seller give each other feedback. The two main ideas behind reputation systems are that, first, it is used to serve as an incentive for good behavior to avoid the negative consequences a bad reputation can entail. Second, it provides a basis for the choice of prospective transaction partners. The relevant properties of a reputation system are discussed in the next sections.

The terms *reputation* and *trust* have been used for various concepts, also synonymously. We define reputation here to mean the performance of a node in participating in the base protocol as seen by others. For mobile ad hoc networking this means participation in routing and forwarding. By trust we mean the performance of a node in the policing protocol that protects the base protocol, here reliability as a witness to provide honest reports.

The use of second-hand information (i.e., reputation information obtained from others) enables nodes to find out about misbehaving nodes before having a bad experience. Also, in mobile ad hoc networks nodes might not meet every node they need for multihop forwarding, but with second-hand information they can make informed decisions about which nodes to use for their paths.

Response

Detection and reputation systems aim at isolating nodes that are deemed misbehaving by not using them for routing and forwarding, and most also isolate them additionally by denying them service. This isolation has three purposes. The first is to reduce the effect of misbehavior by depriving the misbehaving node of the opportunity to participate in the network. The second is to serve as an incentive to behave well to not be denied service. Finally, the third is to obtain better service by not using misbehaving nodes on the path. The isolation is done by each node autonomously, without consensus or human intervention.

Monitoring, reputation, and response come at the price of overhearing transmissions of others, keeping a reputation rating about nodes of interest, and updating it at each observation. The gain can be measured in increased throughput and decreased number of lost packets (i.e., needless transmissions) [1]. Note that the cost, in terms of battery use, of transmissions is much higher than that of simple computations. Nodes have to listen to traffic anyway to find out whether it is for them.

Approaches for Detection and Reputation Systems

The following approaches aim at protecting Dynamic Source Routing (DSR) [6], a reactive routing protocol for mobile ad hoc networks. Briefly, it works as follows. Nodes send out a ROUTE REQUEST (RREQ) message; all

nodes that receive it forward it to their neighbors and put themselves into the source route. If a receiving node is the destination or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. After receiving one or several routes, the source picks the best (by default the shortest), stores it, and sends messages along that path. In case of a link failure, the detecting node sends an error (RERR) toward the source.

Watchdog and Pathrater

Marti, Giuli, Lai, and Baker [2] consider nonforwarding. They call the monitoring part *watchdog*, and the combined reputation and response part *path rater*. The watchdog detects nonforwarding by overhearing the transmission of the next node. Once misbehavior is detected, the source of the concerned path is informed. For reputation, ratings are kept about every node in the network, and the rating of actively used nodes is updated periodically. Nodes select routes with the highest average node rating. The two components enable nodes to avoid misbehaving nodes in their routes as a response. This way, network throughput increases over normal DSR. The response part, in contrast to most other detection and reputation systems (and all others in this article), does not punish misbehaving nodes that do not cooperate, but rather relieves them of forwarding for others, whereas their messages continue to be forwarded.

CONFIDANT

Our own contribution to detection and reputation systems is called CONFIDANT, short for Cooperation Of Nodes, Fairness in Dynamic Ad Hoc Networks, with an initial version with predetermined trust [1], superseded by an adaptive Bayesian reputation and trust system [7]. Nodes monitor their neighborhood and detect several kinds of misbehavior, as listed earlier, by means of an enhanced PACK mechanism [4]. Nodes also gather second-hand information from others and cope with spurious ratings. By Bayesian estimation, nodes classify others as misbehaving or normal. Accordingly, nodes exclude misbehaving nodes from the network as a response, by both avoiding them for routing and denying them cooperation, so that misbehavior will not pay off but results in isolation and thus cannot continue.

CORE

Michiardi and Molva [8] proposed a collaborative reputation (CORE) mechanism that also has a watchdog component for monitoring; it is complemented by a reputation mechanism that differentiates between subjective reputation (observations), indirect reputation (positive reports by others), and functional reputation (task-specific behavior), which are weighted for a combined reputation value that is used to make decisions about cooperation or gradual isolation of a node. Reputation values are obtained by regarding nodes as requesters and providers, and comparing the expected result to the actually obtained result of a request. Nodes only exchange positive reputation information.

Context-Aware Detection

With this mechanism by Paul and Westhoff [9], accusations of nodes are related to the context of a unique route discovery process and a stipulated time period. For monitoring, a combination is used that consists of unkeyed hash verification of routing messages and the detection of misbehavior by comparing a cached routing packet to overheard packets, thereby detecting tampering of the RREQ header. In contrast to watchdog and pathrater, several types of misbehavior are detected. The decision of how to treat nodes in the future, the response, is based on accusations of others, whereby a number of accusations pointing to a single attack, approximate knowledge of the topology, and context-aware inference enable a node to rate an accused node. Accusations are sent to the source, which infers based on majority voting and can inform trusted nodes.

SORI

The Secure and Objective Reputation-Based Incentive (SORI) scheme was proposed by He, Wu, and Khosla [10]; it targets the nonforwarding misbehavior type and uses a watchdog-like mechanism for monitoring. The reputation system keeps count of the packets forwarded both by and for neighboring nodes. Reputation ratings consist of the ratio of these counts, taking into account the confidence in the rating proportional to the number of packets requested for forwarding. Nodes propagate reputation ratings locally; this secondhand information is weighted by credibility, which is derived from the ratio above. The response is given by packet dropping with a probability determined by reputation. SORI additionally employs hash-chain-based authentication for propagated reputation ratings.

Features and Functions of Reputation Systems

The main goal of a reputation system for mobile ad hoc networks is to make sense of gathered information about the behavior of others. We classify the features of a reputation system as follows:

- Representation of information and classification. These determine how monitored events are stored and translated into reputation ratings, and how ratings are classified for response.
- Use of second-hand information. Reputation systems can either rely exclusively on their own observations or also consider information obtained by others. Second-hand information can, however, be spurious, which raises the questions of how to incorporate it in a safe way and whether to propagate it.
- Trust. The use of trust influences the decision of using second-hand information. The design choices are about how to build trust, out-of-band trust vs. building trust on experience, how to represent trust, and how to manage the influence of trust on responses.

Nodes exclude misbehaving nodes from the network as a response, by both avoiding them for routing and denying them cooperation, so that misbehavior will not pay off but results in isolation and thus cannot continue.

The use of trust influences the decision of using first or second-hand information. The design choices are about how to build trust, out-of-band trust versus building trust on experience, how to represent trust, and how to manage the influence of trust on responses.

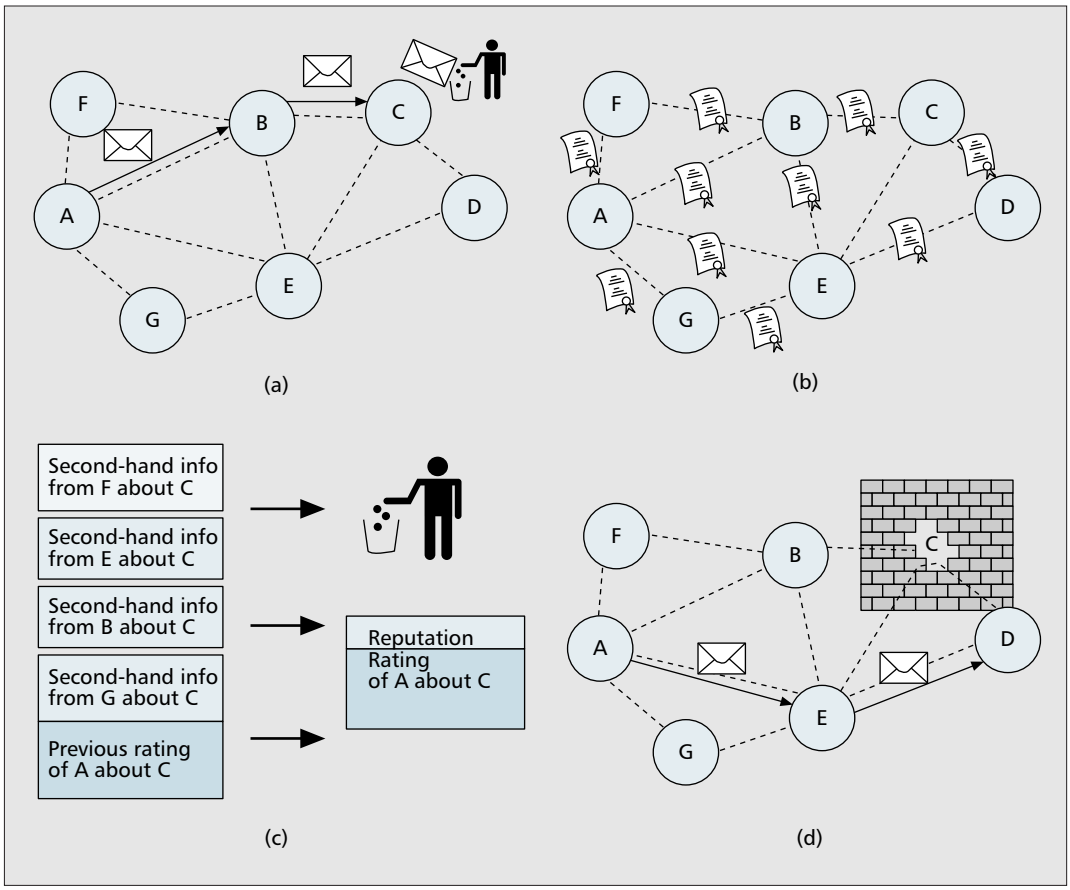

Figure 1. *Misbehavior scenario, node A's view of the network: a) B misbehaves; b) nodes publish first-hand information; c) A rates C; d) A isolates C.*

- Redemption and secondary response. When a node has been isolated, it can no longer be observed. The question of how those nodes should be rated over time is addressed by these two features. If the misbehavior of a node is temporary, a redemption mechanism ensures that it can come back to the network. It is, however, desirable to prevent recidivists from exploiting a redemption mechanism. This can be achieved by secondary response, meaning a quicker response to a recurring threat, in analogy to the human immune system.

We explore these features in the following sections, using a description of how they are implemented in CONFIDANT as a basis for comparison.

Representation of Information and Classification

CONFIDANT uses a Bayesian approach in which the belief of a node i about another node j, as captured in the reputation rating, is updated at each observation to estimate the true but unknown probability of misbehavior θ. Nodes are classified as *misbehaving* when the expected value of θ exceeds a misbehavior tolerance threshold, and as *normal* otherwise. To update ratings, node i keeps a record of first-hand information on node j, called $F_{i,j}$ which has the form (α, β), as parameters to the Beta function for estimating θ. Let $s = 1$ with misbehavior, $s = 0$ otherwise. Then

$$\alpha := u\alpha + s \quad (1)$$

$$\beta := u\beta + (1 - s). \quad (2)$$

The weight u is a discount factor for past experiences. In addition, during inactivity periods the values of α, β periodically decay as follows. Whenever the inactivity time expires, $\alpha := u\alpha$ and $\beta := u\beta$. This is to allow for redemption even in the absence of observations, as explained later.

The approach is illustrated as a scenario in Fig. 1. Node A sends packets via nodes B and C to destination D. For every packet, nodes keep track of the behavior of the next-hop node and remember whether it has forwarded the packet correctly. A stores ratings about B, B about C, and so on.

Suppose that C misbehaves by dropping the packet instead of forwarding it, as shown in Fig. 1a. B's rating of C then becomes bad. Once A classifies C as misbehaving, it also isolates it from the network.

CORE represents reputation values in a reputation table, with separate entries for each node and each function. The reputation values have a range of [–1; 1], 0 being the neutral value. The reputation table captures subjective reputation, indirect reputation, and functional reputation separately; the overall reputation is a function of the previous. Pathrater keeps one rating per node, initially set to 0.5, which is incremented at periodic intervals of 200 ms, decremented by 0.05 when a link break is detected and by 100 upon

misbehavior. The rating range of normal nodes is [0; 0:8]. Context-aware detection has a format for accusation messages and focuses on the inference of misbehavior, which does not depend on reputation representation. SORI keeps counters for the number of packets requested for forwarding and those actually forwarded, and a reputation rating calculated from these counts along with derived confidence and credibility metrics.

Use of Second-Hand Information

In the scenario, since A is not in range with C, it cannot directly observe its behavior and thus cannot detect C's misbehavior. This is solved by allowing the use of second-hand information. In CONFIDANT, in addition to keeping track of direct local observation, nodes publish, as shown in Fig. 1b, their first-hand information from time to time by local broadcasts to exchange information with other nodes. The published information from others is called second-hand information. It is not propagated further. Nodes rely mostly on local information, but they can also take into account the local information of other nodes to gradually get a global view of the network. A thus receives information from its neighbors, here E, F, G, and B, about other nodes, including C. Again, since A has no first-hand information about C in our scenario, it can only find out about C's misbehavior by second-hand information. There is, however, a problem since second-hand information can be spurious (e.g., false accusations). There is a trade-off between the detection speed gained by second-hand information (detection before encounter) and the classification vulnerability introduced.

CONFIDANT has a combination of two mechanisms to cope with spurious second-hand information. First, only compatible secondhand information is considered; that is, information $F_{k,j}$ that does not deviate more than a positive constant d from the expected θ of $R_{i,j}$, as determined by a deviation test:

$$|\mathbb{E}(\text{Beta}(\alpha_F, \beta_F)) - E(\text{Beta}(\alpha, \beta))| \geq d. \qquad (3)$$

If the test is positive, the first-hand information $F_{k,j}$ is considered incompatible by i and discarded. Otherwise, $F_{k,j}$ is incorporated into $R_{i,j}$ such that $R_{i,j} := R_{i,j} + wF_{k,j}$. This is a modified Baysian linear pool model merging, where w is a small constant to weight second-hand information. Second, even when second-hand information is compatible, it is only allowed to slightly influence the reputation rating, determined by the weight w.

Before taking into account this second-hand information to form A's reputation rating about C, A therefore checks whether the second-hand information is compatible with the reputation rating it already has about C. As shown in Fig. 1c, assume that E and G also had bad experiences with C, so B, E, and G are compatible with A's accumulated reputation rating for C. Node F, however, praises C as well behaving, thus deviating substantially from node A's rating. A will let E's, G's, and B's second-hand information slightly influence its reputation rating about C, but it will not consider the second-hand information received from F.

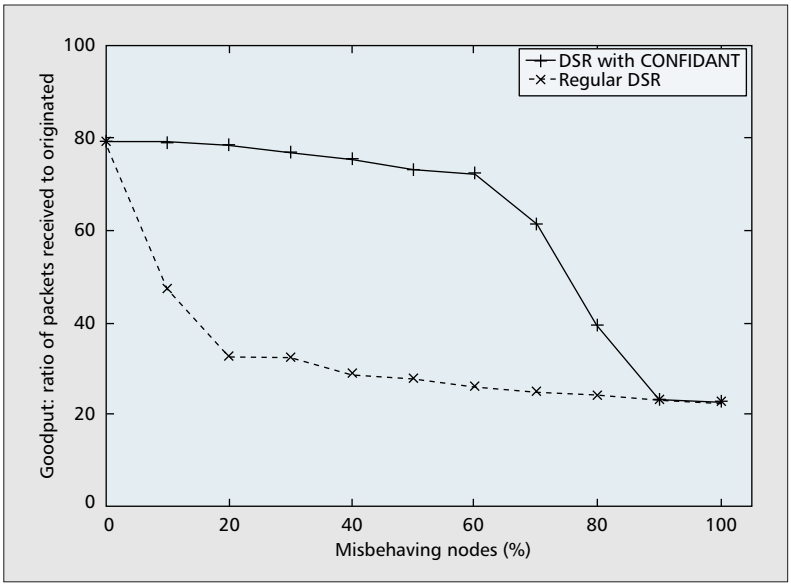

Figure 2. *Goodput, 50 nodes, 30 applications, 0 pause time in random waypoint, varying percentage of misbehaving nodes.*

In Pathrater, nodes send notifications of detected misbehavior to the source of the route, where false accusations are addressed. CORE permits only positive second-hand information, which protects it from spurious accusations but not spurious positive ratings by colluding nodes. Context-aware detection accepts negative second-hand information when at least four separate sources make such a claim; otherwise, the node spreading the information is considered misbehaving. While this inadvertently serves as a disincentive to share ratings, it is robust to spurious accusations by single nodes or small collusions. SORI also exploits the detection speedup by using second-hand information broadcast locally and considers it using a credibility metric, which itself is based on the ratio of requested to actually forwarded packets.

Trust

The main benefit of using trust is to accelerate the detection of misbehaving nodes, and hence the response, by also taking into account incompatible information in a safe way.

In the initial version of CONFIDANT [1], a predetermined trust mechanism similar to the trust management in Pretty Good Privacy (PGP) for key validation and certification was used for trust management for routing and forwarding. When either the source of an accusation was fully trusted or several partially trusted nodes reported the same and their respective assigned trust added up to a value of one entirely trusted node or more, it was considered evidence.

To be robust against trusted yet untrustworthy nodes, CONFIDANT now uses adaptive trust without predetermined ratings, where trust $T_{i,j}$ is based on node i's experience of how honest node j is (i.e., whether the reported first-hand information published by node j is likely to be true). Trust ratings are used to speed up detection by allowing second-hand information coming from a trustworthy node to be accepted without checking for deviation; they are generat-

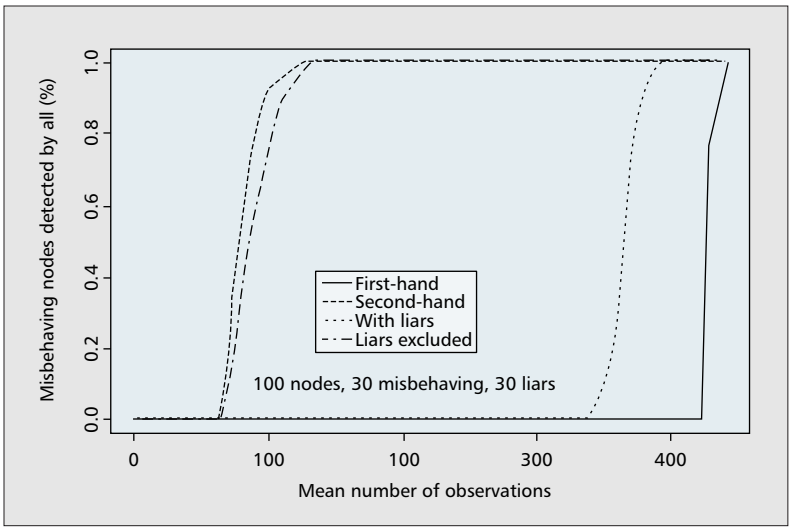

Figure 3. *Mean time for misbehavior detection by all nodes.*

ed automatically by keeping track of the results of the deviation test and updating in analogy to the reputation ratings. In our scenario as depicted in Fig. 1, A improves the trust rating it has about E and B, and worsens the one about F.

SORI bases trust in second-hand information on the forwarding behavior; the other schemes do not have a notion of trust and just accept information from others.

Redemption and Secondary Response

To put more emphasis on recent behavior, CONFIDANT nodes discount all ratings periodically and upon observation by exponential decay; we call this *fading*. This way, nodes cannot capitalize on previous good behavior, and it provides a means of redemption. It is useful to allow redemption of isolated nodes that are no longer misbehaving (e.g., when a bug of a formerly faulty node has been fixed).With fading, the reputation of an isolated node will eventually become tolerable even when no direct observation is possible due to its isolation. If, however, the node misbehaves, it will be isolated again even faster than before. This is achieved by keeping track of which nodes have misbehaved in the past and providing a secondary response by lowering the misbehavior tolerance threshold.

In CORE an isolated node should be redeemed if it behaves well again, but since it cannot prove itself when isolated, it remains isolated. Pathrater suggests a resetting of reputation to the neutral value after a timeout or, alternatively, a slow periodic increase of reputation. Context-aware detection and SORI have no redemption or secondary response.

Sample Scenarios

Misbehavior without Liars

The most common scenario for performance evaluation of detection and reputation systems has been a mobile ad hoc network where some nodes misbehave by dropping packets they should forward for others. All the approaches discussed here have observed increased network performance, despite the presence of misbehaving nodes, over that of normal defenseless networks. Figure 2 shows the effect of CONFIDANT on the ratio of received to originated packets obtained in simulation. The parameters of the reputation system are $u = 0.99$, $w = 0.1$, $d = 0.5$. A comparison of detection speed when relying exclusively on first-hand observations vs. taking into account second-hand information was made in CONFIDANT and SORI. The results indicate that second-hand information considerably speeds up the detection of misbehaving nodes. For an example of CONFIDANT, see Fig. 3.

Misbehavior with Liars

In this scenario nodes not only misbehave in forwarding (and routing), but also in the reputation system itself, by spreading spurious ratings. Given an honest majority of nodes, context-aware detection can cope with its voting scheme, and CONFIDANT is made robust by insisting on compatible ratings [7]. Even with liars, the use of second-hand information decreases the detection time for triggering a response. Figure 3 shows how second-hand information speeds up misbehavior detection. Note that the "liars excluded" line (i.e., the use of CONFIDANT to discard spurious ratings) leads to performance close to that of honest second-hand information. The line "with liars" means that all second-hand information is believed, and we see that spurious ratings degrade performance.

A theoretical analysis of this scenario was done in [11]. It is found that there is a critical value p_c for the probability p that a report originates from a liar. As long as $p < p_c$, the reputation system eliminates the lies. If $p > p_c$, intoxication is possible (see below). With the parameters in Fig. 2, $p_c \approx 1/1 + w$, where w is the discount factor for second-hand information.

Liar Strategies

Untrustworthy nodes can have different strategies to publish their falsified first-hand information when attempting to influence reputation ratings (e.g., when they want to discredit regular nodes). The basic strategies are changing reported misbehavior instances, reported regular behavior, both, mixed, or applied only occasionally.

If the lies are big, they will not pass the deviation test of CONFIDANT. A more sophisticated alternative is stealthy lies. Although nodes do not know the content of the reputation ratings held by others, they could try to infer from published first-hand information and then lie only enough to just pass the deviation test. Even then, the impact is very small as it only differs slightly from what a node already thinks and is further reduced by fading. CORE does not consider negative ratings, so only flattering has an impact. SORI is vulnerable to liars that are cooperative when forwarding. Context-aware detection copes with single liars or very small collusions by majority voting. Pathrater has no defense against liars.

BRAINWASHING

When a node is surrounded by colluding lying nodes, it can be tricked into believing false information. When it later moves into a different neighborhood with honest nodes, it will not believe them since their information deviates too much from its own. We call this being brainwashed. Neither SORI, context-aware detection, nor CONFIDANT prevent brainwashing by collusion, but in CONFIDANT the ratings over time will return to neutral by fading and the node can recover. As an aside, if a node is surrounded by misbehaving nodes, cooperation cannot be guaranteed in any case since there is no benign alternative for the first hop of a route.

INTOXICATION

When trust is adapted to experience as in CONFIDANT, if nodes use the trust option to allow incompatible second-hand information to be used in order to speed up detection, nodes could try to gain trust from others by telling the truth over a sustained period of time and only then start lying. We call this intoxication; it is mitigated by two properties in CONFIDANT. First, fading discounts trust gained in the past, and recent deviations reduce trust more strongly. Second, in telling the truth or publishing whichever information passes the deviation test, they actually reinforce the reputation ratings other nodes have, making it harder to get their then deviating information accepted.

Intoxication can also occur in systems that rely on out-of-band or predetermined trust, such as the initial CONFIDANT, since nodes can change their behavior even after they have been classified as trusted. Unless trust ratings are adaptive, such systems remain vulnerable. The trust rating, however, needs to be adaptive to the trust performance itself; otherwise, if it is adaptive to other behavior as in SORI, lying nodes are not caught.

IDENTITY SPOOFING

The question of identity is central to reputation systems. Without identity persistence, a badly rated node could disappear and reappear with a different identity. For a reputation system to be useful, the identity has to persist longer than the detection time of a misbehaving node. We show in Fig. 3 that the time needed for all misbehaving nodes (nonforwarding) to be detected as such by all other nodes in a network of 100 nodes, given mobility, is on the order of 100 packets and much less for local detection [12]. One way of achieving identity persistence is by expensive pseudonyms. In the scenario where the mobile ad hoc network is not completely cut off from the Internet, we can make use of certification authorities. Other possible ways of providing identity are tamper-proof hardware or radio signal watermarking.

CONCLUSIONS

We have shown in this article how reputation systems for self-policing and adaptation to network cooperation can be built, and how they can mitigate the deleterious effects of misbehavior in self-organized networks by using monitoring to generate reputation ratings which in turn allow nodes to make informed decisions about their response to the behavior of other nodes. We have described how second-hand information can be used to improve the response, while avoiding the dangers of rumor spreading. Our survey suggests that a reputation system is effective as long as the number of misbehaving nodes is not too large; it would be interesting to understand this point theoretically.

The question of identity is central to reputation systems. Without identity persistence, a badly rated node could disappear and reappear with a different identity. For a reputation system to be useful, the identity has to persist longer than the detection time of a misbehaving node.

REFERENCES

[1] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes — Fairness In Dynamic Ad-hoc Networks," *Proc. IEEE/ACM Symp. Mobile Ad Hoc Net. and Comp.*, Lausanne, Switzerland, June 2002.
[2] S. Marti *et al.*, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. MOBICOM 2000*, 2000, pp. 255–65.
[3] L. Buttyan and J.-P. Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks," *ACM Mobile Comp. and Commun. Rev.*, Oct. 2002.
[4] S. Buchegger, C. Tissieres, and J.-Y. Le Boudec, "A Testbed for Misbehavior Detection in Mobile Ad Hoc Networks," *Proc. IEEE WMCSA 2004*, U.K., Dec. 2004.
[5] J.-Y. Le Boudec and S. Sarafijanovic, "An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad Hoc Networks," *Proc. Bio-ADIT 2004*, Lausanne, Switzerland, Jan. 2004.
[6] Y. Hu, D. Johnson, and D. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (dsr)," http://www.ietf.org/internetdrafts/ draft-ietf-manet-dsr-09.txt, Apr. 2003.
[7] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for Peer-to-Peer and Mobile Ad Hoc Networks," *P2PEcon*, Harvard Univ., Cambridge, MA, June 2004.
[8] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *6th IFIP Conf. Sec. Commun. and Multimedia*, Portoroz, Slovenia, 2002.
[9] K. Paul and D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks," *Proc. IEEE GLOBECOM*, Taipeh, Taiwan, 2002, IEEE.
[10] Q. He, D. Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad Hoc Networks," *WCNC 2004*, Atlanta, GA, Mar. 2004.
[11] J. Mundinger and J.-Y. Le Boudec. Analysis of a Reputation System for Mobile Ad-hoc Networks with Liars," *Proc. 3rd Int'l. Symp. Modeling and Optimization*, Trento, Italy, April 2005.
[12] S. Buchegger and Jean-Yves Le Boudec, "The Effect of Rumor Spreading in Reputation Systems in Mobile Ad Hoc Networks," *Wiopt'03*, Sofia-Antipolis, Mar. 2003.

BIOGRAPHIES

SONJA BUCHEGGER [SM'96, M'05] is a post-doctoral scholar at the University of California at Berkeley, School of Information Management and Systems. She received her Ph.D. in communication systems from EPFL, Switzerland, in 2004, a graduate degree in computer science in 1999, and undergraduate degrees in computer science in 1996 and business administration in 1995 from the University of Klagenfurt, Austria. In 2003 and 2004 she was a research and teaching assistant at EPFL, and from 1999 to 2003 she worked at the IBM Zurich Research Laboratory in the Network Technologies Group. Her current research interests are mobile ad hoc and peer-to-peer network economics and security.

JEAN-YVES LE BOUDEC [M'89] is a full professor at EPFL. He graduated from Ecole Normale Superieure de Saint-Cloud, Paris, where he obtained the Agregation in Mathematics (rank 4) in 1980. He received his doctorate in 1984 from the University of Rennes, France, and became an assistant professor at INSA/IRISA, Rennes. In 1987 he joined Bell Northern Research, Ottawa, Canada, as a member of scientific staff in the Network and Product Traffic Design Department. In 1988 he joined the IBM Zurich Research Laboratory where he was manager of the Customer Premises Network Department. In 1994 he formed the Laboratoire de Reseaux de Communication at EPFL. His interests are in the architecture and performance of communication systems.